09/936570
JC16 Rec'd PCT/PTO SEP 14 2001

PATENT
2565-0236P

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	SORIMACHI, Toru et al.	Conf.:	
Int'l. Appl. No.:	PCT/JP00/09129		
Appl. No.:	NEW	Group:	
Filed:	September 14, 2001	Examiner:	
For:	ENCRYPTOR, ENCRYPTING METHOD, DECRYPTOR, DECRYPTING METHOD, AND COMPUTER READABLE RECORDING MEDIUM HAVING PROGRAM STORED THEREIN		

PRELIMINARY AMENDMENT

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, DC 20231

September 14, 2001

Sir:

The following Preliminary Amendments and Remarks are respectfully submitted in connection with the above-identified application.

AMENDMENTS

IN THE SPECIFICATION:

Please amend the specification as follows:

Before line 1, insert --This application is the national phase under 35 U.S.C. § 371 of PCT International Application No. PCT/JP00/09129 which has an International filing date of December 22, 2000, which designated the United States of America and was not published in English.--

Please replace the first paragraph on page 45, lines 3-25 continuing on page 46 lines 1-6, with the following rewritten paragraph:

--At time T0, the key K_1 is supplied from the outside as the key KI. As the switch 157 is connected to E, the key K_1 is stored in the register 156. Then, the encrypting process for the plaintext block data M_1 is started. When the plaintext block data M_1 is started at time T0, the selector 54 inputs an initial value IV through A, and then the selector 54 is switched to B. At time X during the encrypting process of the plaintext block data M_1 using the key K_1, it is assumed that the interrupt IT for requesting to encrypt the plaintext block data N_1. Until time T1, the ciphertext block data C_1 becomes stored in the memory 55. Then, the key K_2 is supplied to the encrypting module 51 from the outside as the key KI at time T1 due to the generation of the interrupt IT. At time T1, the input to the selector 54 is set to A. And at time T1, the switch 57 and the switch 157 are connected to F. Accordingly, the key K_2 is not stored in the register 156. After time T1, the encryption of the plaintext block data N_1 is performed using the key K_2, and the ciphertext block data D_1 is output. At time Y, the encryption of the plaintext block data N_1 is finished, and the interrupt IT is resolved. Due to this resolution of the interrupt IT, at time T2, the input to the selector 54 is switched to C, and the switch 57 is connected to E. Consequently, the key K_1 is output to the

selector 154 from the register 156 as the key KI, and the key K_1 is supplied to the encrypting module 51 from the selector 154 as the key K_1. Further, as the selector 54 is switched to C, the ciphertext block data C_1 stored in the memory 55 is input for encrypting the plaintext block data M_2, the plaintext block data M_2 is encrypted by the encrypting module 51 using the key K_1, and the ciphertext block data C_2 is output. Before time T3, the input to the selector 54 is switched to B, and when the plaintext block data M_3 is encrypted, the ciphertext block data C_2 fed back from the feedback line 65 of the feedback loop is input, the plaintext block data M_3 is encrypted by the encrypting module 51 using the key K_1, and the ciphertext block data C_3 is output.--

Please replace the second paragraph on page 57, lines 12-25 continuing on page 58 lines 1-2, with the following rewritten paragraph:

--Fig. 37 shows the encryptor which encrypts the plaintext data including at least one plaintext block data using the encrypting module and generates the MAC for ensuring the integrity of the ciphertext data. The encryptor includes an encrypting unit 100 having a first feedback loop 65 which feeds back the ciphertext block data C_i output from the encrypting module 51 at encrypting time of the plaintext block data by the encrypting unit 52. The encrypting unit 100 inputs the plaintext block data M_i, makes the ciphertext block data C_i feedback using the first feedback loop 65 to perform the encrypting process, and

outputs the ciphertext block data C_i. The encryptor further includes a MAC generator 200 having a second feedback loop 66 which feeds back a computed intermediate MAC result T_i. The MAC generator 200 inputs the ciphertext block data C_i at every output of the ciphertext block data C_i from the encrypting unit 100, computes the MAC, makes the computed intermediate MAC result T_i feedback using the second feedback loop 66, and generates a MAC P to ensure the integrity of the ciphertext data.--

Docket No. 2565-0236P

REMARKS

The specification has been amended to provide a cross-reference to the previously filed International Application. The specification has also been amended to correct typographical errors.

Entry of the above amendments is earnestly solicited. An early and favorable first action on the merits is earnestly solicited.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By _____ #34,313
John A. Castellano, #35,094

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

JAC/rem
2565-0236P

Attachment: VERSION WITH MARKINGS TO SHOW CHANGES MADE